# THE ENDOMORPHISM RINGS OF JACOBIANS OF CYCLIC COVERS OF THE PROJECTIVE LINE 

BY YURI G. ZARHIN $\dagger$<br>Department of Mathematics, Pennsylvania State University,<br>University Park, PA 16802,USA<br>e-mail: zarhin@math.psu.edu


#### Abstract

Suppose $K$ is a field of characteristic zero, $K_{a}$ is its algebraic closure, $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$, whose Galois group coincides either with the full symmetric group $\mathbf{S}_{n}$ or with the alternating group $\mathbf{A}_{n}$. Let $p$ be an odd prime, $\mathbf{Z}\left[\zeta_{p}\right]$ the ring of integers in the $p$ th cyclotomic field $\mathbf{Q}\left(\zeta_{p}\right)$. Suppose $C$ is the smooth projective model of the affine curve $y^{p}=f(x)$ and $J(C)$ is the jacobian of $C$. We prove that the ring $\operatorname{End}(J(C))$ of $K_{a}$-endomorphisms of $J(C)$ is canonically isomorphic to $\mathbf{Z}\left[\zeta_{p}\right]$.


## 1. Introduction

We write $\mathbf{Z}, \mathbf{Q}, \mathbf{C}$ for the ring of integers, the field of rational numbers and the field of complex numbers respectively. Recall that a number field is called a CMfield if it is a purely imaginary quadratic extension of a totally real field. Let $p$ be an odd prime, $\zeta_{p} \in \mathbf{C}$ a primitive $p$ th root of unity, $\mathbf{Q}\left(\zeta_{p}\right) \subset \mathbf{C}$ the $p$ th cyclotomic field and $\mathbf{Z}\left[\zeta_{p}\right]$ the ring of integers in $\mathbf{Q}\left(\zeta_{p}\right)$. It is well-known that $\mathbf{Q}\left(\zeta_{p}\right)$ is a CM-field of degree $p-1$. We write $\mathbf{F}_{p}$ for the finite field consisting of $p$ elements.

Let $f(x) \in \mathbf{C}[x]$ be a polynomial of degree $n \geq 4$ without multiple roots. Let $C_{f, p}$ be a smooth projective model of the smooth affine curve

$$
y^{p}=f(x)
$$

It is well-known that the genus $g\left(C_{f, p}\right)$ of $C_{f, p}$ is $(p-1)(n-1) / 2$ if $p$ does not divide $n$ and $(p-1)(n-2) / 2$ if it does. The map

$$
(x, y) \mapsto\left(x, \zeta_{p} y\right)
$$

$\dagger$ Partially supported by the NSF.
gives rise to a non-trivial birational automorphism

$$
\delta_{p}: C_{f, p} \rightarrow C_{f, p}
$$

of period $p$.
The jacobian $J^{(f, p)}:=J\left(C_{f, p}\right)$ of $C_{f, p}$ is an abelian variety of dimension $g\left(C_{f, p}\right)$. We write $\operatorname{End}\left(J^{(f, p)}\right)$ for the ring of endomorphisms of $J^{(f, p)}$ over C. By Albanese functoriality, $\delta_{p}$ induces an automorphism of $J^{(f, p)}$ which we still denote by $\delta_{p}$; it is known (10, p. 149], 11, p. 458]) that

$$
\delta_{p}^{p-1}+\cdots+\delta_{p}+1=0
$$

in $\operatorname{End}\left(J^{(f, p)}\right)$. This gives us an embedding

$$
\mathbf{Z}\left[\zeta_{p}\right] \cong \mathbf{Z}\left[\delta_{p}\right] \subset \operatorname{End}\left(J^{(f, p)}\right)
$$

(10, p. 149], [11, p. 458]).
Our main result is the following statement.
Theorem 1.1. Let $K$ be a subfield of $\mathbf{C}$ such that all the coefficients of $f(x)$ lie in $K$. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \geq 5$ and its Galois group over $K$ is either the symmetric group $\mathbf{S}_{n}$ or the alternating group $\mathbf{A}_{n}$. Then

$$
\operatorname{End}\left(J^{(f, p)}\right)=\mathbf{Z}\left[\delta_{p}\right] \cong \mathbf{Z}\left[\zeta_{p}\right]
$$

In particular, $J^{(f, p)}$ is a simple complex abelian variety.

Remark 1.2. In the case when $p$ is a Fermat prime the assertion of Theorem 1.1 is proven in 20. (Also in 20] the author proved that if the conditions of Theorem 1.1 hold true then $\mathbf{Z}\left[\delta_{p}\right]$ is a maximal commutative subring in $\operatorname{End}\left(J^{(f, p)}\right)$ for all odd primes $p$. See 21 for a similar result in positive characteristic when $p \mid n$ and $n \geq 9$.) The "opposite" case when $J^{(f, p)}$ is an abelian variety of CM-type was studied in [2]. An analogue of Theorem 1.1 for hyperelliptic jacobians (i.e., the case of $p=2$ ) was proven in (17) (see also 18], 19]).

Examples 1.3. (1) the polynomial $x^{n}-x-1 \in \mathbf{Q}[x]$ has Galois group $\mathbf{S}_{n}$ over $\mathbf{Q}([13$, p. 42]). Therefore the endomorphism ring (over $\mathbf{C})$ of the jacobian $J(C)$ of the curve $C: y^{p}=x^{n}-x-1$ is $\mathbf{Z}\left[\zeta_{p}\right]$ if $n \geq 5$.
(2) the Galois group of the "truncated exponential"

$$
\exp _{n}(x):=1+x+\frac{x^{2}}{2}+\frac{x^{3}}{6}+\cdots+\frac{x^{n}}{n!} \in \mathbf{Q}[x]
$$

is either $\mathbf{S}_{n}$ or $\mathbf{A}_{n}$ 12. Therefore the endomorphism ring (over $\mathbf{C}$ ) of the jacobian $J(C)$ of the curve $C: y^{p}=\exp _{n}(x)$ is $\mathbf{Z}\left[\zeta_{p}\right]$ if $n \geq 5$.

Remark 1.4. If $f(x) \in K[x]$ then the curve $C_{f, p}$ and its jacobian $J^{(f, p)}$ are defined over $K$. Let $K_{a} \subset \mathbf{C}$ be the algebraic closure of $K$. Clearly, all endomorphisms of $J^{(f, p)}$ are defined over $K_{a}$. This implies that in order to prove Theorem 1.1, it suffices to check that $\mathbf{Z}\left[\delta_{p}\right]$ coincides with the ring of all $K_{a}$-endomorphisms of $J^{(f, p)}$ or equivalently, that $\mathbf{Q}\left[\delta_{p}\right]$ coincides with the $\mathbf{Q}$-algebra of $K_{a}$-endomorphisms of $J^{(f, p)}$.

The paper is organized as follows. Section 2 contains auxiliary results about endomorphism algebras of complex abelian varieties. We use them in Section 33 in order to study endomorphisms of $J^{(f, p)}$. In Section $⿴$ we prove the main result. The short last Section contains corrigendum to 20].

The author would like to thank the referee for useful comments.

## 2. Complex abelian varieties

Throughout this section we assume that $Z$ is a complex abelian variety of positive dimension. As usual, we write $\operatorname{End}^{0}(Z)$ for the semisimple finite-dimensional Qalgebra $\operatorname{End}(Z) \otimes \mathbf{Q}$. We write $\mathfrak{C}_{Z}$ for the center of $\operatorname{End}^{0}(Z)$. It is well-known that $\mathfrak{C}_{Z}$ is a direct product of finitely many number fields. All the fields involved are either totally real number fields or CM-fields. Let $H_{1}(Z, \mathbf{Q})$ be the first rational homology group of $Z$; it is a $2 \operatorname{dim}(Z)$-dimensional $\mathbf{Q}$-vector space. By functoriality $\operatorname{End}^{0}(Z)$ acts on $H_{1}(Z, \mathbf{Q})$; hence we have an embedding

$$
\operatorname{End}^{0}(Z) \hookrightarrow \operatorname{End}_{\mathbf{Q}}\left(H_{1}(Z, \mathbf{Q})\right)
$$

(which sends 1 to 1 ).
Suppose $E$ is a subfield of $\operatorname{End}^{0}(Z)$ that contains the identity map. Then $H_{1}(Z, \mathbf{Q})$ becomes an $E$-vector space of dimension

$$
d=\frac{2 \operatorname{dim}(Z)}{[E: \mathbf{Q}]}
$$

We write

$$
\operatorname{Tr}_{E}: \operatorname{End}_{E}\left(H_{1}(Z, \mathbf{Q})\right) \rightarrow E
$$

for the corresponding trace map on the $E$-algebra of $E$-linear operators in $H_{1}(Z, \mathbf{Q})$.

Extending by C-linearity the action of $\operatorname{End}^{0}(Z)$ and of $E$ on the complex cohomology group

$$
H_{1}(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}=H_{1}(Z, \mathbf{C})
$$

of $Z$ we get the embeddings

$$
E \otimes_{\mathbf{Q}} \mathbf{C} \subset \operatorname{End}^{0}(Z) \otimes_{\mathbf{Q}} \mathbf{C} \hookrightarrow \operatorname{End}_{\mathbf{C}}\left(H_{1}(Z, \mathbf{C})\right)
$$

which provide $H_{1}(Z, \mathbf{C})$ with a natural structure of free $E_{\mathbf{C}}:=E \otimes_{\mathbf{Q}}$ C-module of rank $d$. If $\Sigma_{E}$ is the set of embeddings of $\sigma: E \hookrightarrow \mathbf{C}$ then it is well-known that

$$
E_{\mathbf{C}}=E \otimes_{\mathbf{Q}} \mathbf{C}=\prod_{\sigma \in \Sigma_{E}} E \otimes_{E, \sigma} \mathbf{C}=\prod_{\sigma \in \Sigma_{E}} \mathbf{C}_{\sigma}
$$

where

$$
\mathbf{C}_{\sigma}=E \otimes_{E, \sigma} \mathbf{C}=\mathbf{C}
$$

Since $H_{1}(Z, \mathbf{C})$ is a free $E_{\mathbf{C}}$-module of rank $d$, there is the corresponding trace map

$$
\operatorname{Tr}_{E_{\mathbf{C}}}: \operatorname{End}_{E_{\mathbf{C}}}\left(H_{1}(Z, \mathbf{C})\right) \rightarrow E_{\mathbf{C}}
$$

which coincides on $E_{\mathbf{C}}$ with multiplication by $d$ and with $\operatorname{Tr}_{E}$ on $\operatorname{End}_{E}\left(H_{1}(Z, \mathbf{Q})\right)$.
We write $\operatorname{Lie}(Z)$ for the tangent space of $Z$; it is a $\operatorname{dim}(Z)$-dimensional $\mathbf{C}$-vector space. By functoriality, $\operatorname{End}^{0}(Z)$ and therefore $E$ acts on $\operatorname{Lie}(Z)$. This provides $\operatorname{Lie}(Z)$ with a natural structure of $E \otimes_{\mathbf{Q}} \mathbf{C}$-module. We have

$$
\operatorname{Lie}(Z)=\bigoplus_{\sigma \in \Sigma_{E}} \mathbf{C}_{\sigma} \operatorname{Lie}(Z)=\oplus_{\sigma \in \Sigma_{E}} \operatorname{Lie}(Z)_{\sigma}
$$

where

$$
\operatorname{Lie}(Z)_{\sigma}=\mathbf{C}_{\sigma} \operatorname{Lie}(Z)=\{x \in \operatorname{Lie}(Z) \mid e x=\sigma(e) x \quad \forall e \in E\}
$$

Let us put

$$
n_{\sigma}=n_{\sigma}(Z, E)=\operatorname{dim}_{\mathbf{C}_{\sigma}} \operatorname{Lie}(Z)_{\sigma}=\operatorname{dim}_{\mathbf{C}} \operatorname{Lie}(Z)_{\sigma}
$$

We write $\sigma^{\prime}: E \hookrightarrow \mathbf{C}$ for the composition of $\sigma: E \hookrightarrow \mathbf{C}$ and the complex conjugation $\mathbf{C} \rightarrow \mathbf{C}$. The embedding $\sigma^{\prime} \in \Sigma_{E}$ is (called) the complex-conjugate of $\sigma$.

Remark 2.1. It is well-known ([1], p. 53], [5, p. 84]) that

$$
n_{\sigma}+n_{\sigma^{\prime}}=d \quad \forall \sigma \in \Sigma_{E}
$$

Remark 2.2. Let $\Omega^{1}(Z)$ be the space of the differentials of the first kind on $Z$. It is well-known that the natural map

$$
\Omega^{1}(Z) \rightarrow \operatorname{Hom}_{\mathbf{C}}(\operatorname{Lie}(Z), \mathbf{C})
$$

is an isomorphism. This isomorphism allows us to define via duality the natural homomorphism

$$
E \rightarrow \operatorname{End}_{\mathbf{C}}\left(\operatorname{Hom}_{\mathbf{C}}(\operatorname{Lie}(Z), \mathbf{C})\right)=\operatorname{End}_{\mathbf{C}}\left(\Omega^{1}(Z)\right)
$$

This provides $\Omega^{1}(Z)$ with a natural structure of $E \otimes_{\mathbf{Q}} \mathbf{C}$-module in such a way that

$$
\Omega^{1}(Z)_{\sigma}:=\mathbf{C}_{\sigma} \Omega^{1}(Z) \cong \operatorname{Hom}_{\mathbf{C}}\left(\operatorname{Lie}(Z)_{\sigma}, \mathbf{C}\right)
$$

In particular,

$$
n_{\sigma}=\operatorname{dim}_{\mathbf{C}}\left(\operatorname{Lie}(Z)_{\sigma}\right)=\operatorname{dim}_{\mathbf{C}}\left(\Omega^{1}(Z)_{\sigma}\right)
$$

Theorem 2.3. Suppose $E$ contains $\mathfrak{C}_{Z}$. Then the tuple

$$
\left(n_{\sigma}\right)_{\sigma \in \Sigma_{E}} \in \prod_{\sigma \in \Sigma_{E}} \mathbf{C}_{\sigma}=E \otimes_{\mathbf{Q}} \mathbf{C}
$$

lies in $\mathfrak{C}_{Z} \otimes_{\mathbf{Q}} \mathbf{C}$. In particular, if $E / \mathbf{Q}$ is Galois and $\mathfrak{C}_{Z} \neq E$ then there exists a nontrivial automorphism $\kappa: E \rightarrow E$ such that $n_{\sigma}=n_{\sigma \kappa}$ for all $\sigma \in \Sigma_{E}$.

Proof. The inclusion $\mathfrak{C}_{Z} \subset E$ implies that $\mathfrak{C}_{Z}$ is a field.
There is a canonical Hodge decomposition ([7], chapter 1], [1], pp. 52-53])

$$
H_{1}(Z, \mathbf{C})=H^{-1,0} \oplus H^{0,-1}
$$

where $H^{-1,0}$ and $H^{0,-1}$ are mutually "complex conjugate" $\operatorname{dim}(Z)$-dimensional complex vector spaces. This splitting is $\operatorname{End}^{0}(Z)$-invariant and the $\operatorname{End}^{0}(Z)$-module $H^{-1,0}$ is canonically isomorphic to $\operatorname{Lie}(Z)$. Let

$$
\mathfrak{f}_{H}: H_{1}(Z, \mathbf{C}) \rightarrow H_{1}(Z, \mathbf{C})
$$

be the $\mathbf{C}$-linear operator in $H_{1}(Z, \mathbf{C})$ defined as follows.

$$
\mathfrak{f}_{H}(x)=-x \quad \forall x \in H^{-1,0} ; \quad \mathfrak{f}_{H}(x)=0 \quad \forall x \in H^{0,-1}
$$

Clearly, $\mathfrak{f}_{H}$ commutes with $\operatorname{End}^{0}(Z)$ and therefore with $E$. Hence $\mathfrak{f}_{H}$ may be viewed as an endomorphism of the free $E_{\mathbf{C}}$-module $H_{1}(Z, \mathbf{C})$; clearly, its trace is the tuple

$$
\left(-n_{\sigma}\right)_{\sigma \in \Sigma_{E}} \in \prod_{\sigma \in \Sigma_{E}} \mathbf{C}_{\sigma}=E_{\mathbf{C}}
$$

Suppose $M T=M T_{Z} \subset \mathrm{GL}_{\mathbf{Q}}\left(H_{1}(Z, \mathbf{Q})\right)$ ) is the Mumford-Tate group of (the rational Hodge structure $H_{1}(Z, \mathbf{Q})$ and of) $Z(1,9,16)$. It is a connected reductive
algebraic Q-group that contains scalars and could be described as follows (16, section 6.3]). Let $\left.m t \subset \operatorname{End}_{\mathbf{Q}}\left(H_{1}(Z, \mathbf{Q})\right)\right)$ be the $\mathbf{Q}$-Lie algebra of $M T$; it is a reductive algebraic linear Q-Lie algebra which contains scalars and its natural faithful representation in $H_{1}(Z, \mathbf{Q})$ is completely reducible. In addition, $m t$ is the smallest $\mathbf{Q}$-Lie subalgebra in $\left.\operatorname{End}_{\mathbf{Q}}\left(H_{1}(Z, \mathbf{Q})\right)\right)$ enjoying the following property: its complexification

$$
m t_{\mathbf{C}}=m t \otimes_{\mathbf{Q}} \mathbf{C} \subset \operatorname{End}_{\mathbf{C}}\left(H_{1}(Z, \mathbf{C})\right)
$$

contains scalars and $\mathfrak{f}_{H}$. It is well-known that the centralizer of $M T$ (and therefore of $m t)$ in $\operatorname{End}_{\mathbf{Q}}\left(H_{1}(Z, \mathbf{Q})\right)$ coincides with $\operatorname{End}^{0}(Z)$. This implies that the center $\mathfrak{c}$ of $m t$ lies in $\mathfrak{C}_{Z}$. Since $m t$ is reductive, it splits into a direct sum

$$
m t=m t^{s s} \oplus \mathfrak{c}
$$

of $\mathfrak{c}$ and a semisimple $\mathbf{Q}$-Lie algebra $m t^{s s}$. Clearly, $m t$ lies in $\operatorname{End}_{E}\left(H_{1}(Z, \mathbf{Q})\right)$.
Since $m t^{s s}$ is semisimple and the trace map $\operatorname{Tr}_{E}$ is a Lie algebra homomorphism, $\operatorname{Tr}_{E}\left(m t^{s s}\right)=\{0\}$. Since $\mathfrak{c} \subset \mathfrak{C}_{Z} \subset E$, we have $\operatorname{Tr}_{E}(\mathfrak{c}) \subset \mathfrak{C}_{Z}$ and therefore

$$
\operatorname{Tr}_{E}(m t) \subset \mathfrak{C}_{Z}
$$

This implies easily that

$$
\operatorname{Tr}_{E_{\mathbf{C}}}\left(m t_{\mathbf{C}}\right) \subset \mathfrak{C}_{Z} \otimes_{\mathbf{Q}} \mathbf{C}
$$

In particular, since $\mathfrak{f}_{H} \in m t_{\mathbf{C}}$, we have $\operatorname{Tr}_{E_{\mathbf{C}}}\left(\mathfrak{f}_{H}\right) \in \mathfrak{C}_{Z} \otimes_{\mathbf{Q}} \mathbf{C}$. But $\operatorname{Tr}_{E_{\mathbf{C}}}\left(\mathfrak{f}_{H}\right)=$ $\left(-n_{\sigma}\right)_{\sigma \in \Sigma}$. This implies easily that

$$
\left(n_{\sigma}\right)_{\sigma \in \Sigma_{E}}=-\operatorname{Tr}_{E_{\mathbf{C}}}\left(\mathfrak{f}_{H}\right) \in \mathfrak{C}_{Z} \otimes_{\mathbf{Q}} \mathbf{C}
$$

In order to prove the second assertion of the theorem, notice that its assumptions imply that $E / \mathfrak{C}_{Z}$ is a nontrivial Galois extension. If $\kappa: E \rightarrow E$ is a non-identity element of the Galois group $\operatorname{Gal}\left(E / \mathfrak{C}_{Z}\right)$ then one may easily check that

$$
\mathfrak{C}_{Z} \otimes_{\mathbf{Q}} \mathbf{C} \subset\left\{(u)_{\sigma \in \Sigma_{E}} \in \prod_{\sigma \in \Sigma_{E}} \mathbf{C}=E_{\mathbf{C}} \mid u_{\sigma}=u_{\sigma \kappa} \quad \forall \sigma\right\}
$$

## 3. Cyclic covers and jacobians

Throughout this paper we fix an odd prime $p$ and assume that $K$ is a field of characteristic zero. We fix an algebraic closure $K_{a}$ and write $\operatorname{Gal}(K)$ for the absolute Galois group $\operatorname{Aut}\left(K_{a} / K\right)$. We also fix in $K_{a}$ a primitive $p$ th root of unity $\zeta$.

Let $f(x) \in K[x]$ be a separable polynomial of degree $n \geq 4$. We write $\Re_{f}$ for the set of its roots and denote by $L=L_{f}=K\left(\Re_{f}\right) \subset K_{a}$ the corresponding splitting field. As usual, the Galois group $\operatorname{Gal}(L / K)$ is called the Galois group of $f$ and denoted by $\operatorname{Gal}(f)$. Clearly, $\operatorname{Gal}(f)$ permutes elements of $\Re_{f}$ and the natural map of $\operatorname{Gal}(f)$ into the group $\operatorname{Perm}\left(\mathfrak{R}_{f}\right)$ of all permutations of $\mathfrak{R}_{f}$ is an embedding. We will identify $\operatorname{Gal}(f)$ with its image and consider it as a permutation group of $\mathfrak{R}_{f}$. Clearly, $\operatorname{Gal}(f)$ is transitive if and only if $f$ is irreducible in $K[x]$.

We refer the reader to [6, 20, 3, 8] for the definition and properties of the heart $\left(\mathbf{F}_{p}^{\Re_{f}}\right)^{00}$ over the field $\mathbf{F}_{p}$ of the group $\operatorname{Gal}(f)$ acting on the set $\mathfrak{R}_{f}$. Here we just recall that $\left(\mathbf{F}_{p}^{\Re_{f}}\right)^{00}$ is a finite-dimensional $\mathbf{F}_{p}$-vector space provided with a natural structure of $\operatorname{Gal}(f)$-module.

Let $C=C_{f, p}$ be the smooth projective model of the smooth affine $K$-curve

$$
y^{p}=f(x) \text {. }
$$

So $C$ is a smooth projective curve defined over $K$. The rational function $x \in K(C)$ defines a finite cover $\pi: C \rightarrow \mathbf{P}^{1}$ of degree $p$. Let $B^{\prime} \subset C\left(K_{a}\right)$ be the set of ramification points. Clearly, the restriction of $\pi$ to $B^{\prime}$ is an injective map $B^{\prime} \hookrightarrow$ $\mathbf{P}^{1}\left(K_{a}\right)$, whose image is the disjoint union of $\infty$ and $\mathfrak{R}_{f}$ if $p$ does not divide $\operatorname{deg}(f)$ and just $\Re_{f}$ if it does. We write

$$
B=\pi^{-1}\left(\mathfrak{R}_{f}\right)=\left\{(\alpha, 0) \mid \alpha \in \mathfrak{R}_{f}\right\} \subset B^{\prime} \subset C\left(K_{a}\right) .
$$

Clearly, $\pi$ is ramified at each point of $B$ with ramification index $p$. We have $B^{\prime}=B$ if and only if $n$ is divisible by $p$. If $n$ is not divisible by $p$ then $B^{\prime}$ is the disjoint union of $B$ and a single point $\infty^{\prime}:=\pi^{-1}(\infty)$. In addition, the ramification index of $\pi$ at $\pi^{-1}(\infty)$ is also $p$. Using Hurwitz's formula, one may easily compute the genus $g=g(C)=g\left(C_{p, f}\right)$ of $C$ ( 4 pp. 401-402], [14, proposition 1 on p. 3359], 10, p. 148]). Namely, $g$ is $(p-1)(n-1) / 2$ if $p$ does not divide $n$ and $(p-1)(n-2) / 2$ if it does.

Remark 3.1. Assume that $p$ does not divide $n$ and consider the plane triangle (Newton polygon)

$$
\Delta_{n, p}:=\{(j, i) \mid 0 \leq j, \quad 0 \leq i, \quad p j+n i \leq n p\}
$$

with the vertices $(0,0),(0, p)$ and $(n, 0)$. Let $L_{n, p}$ be the set of integer points in the interior of $\Delta_{n, p}$. One may easily check that $g$ coincides with the number of
elements of $L_{n, p}$. It is also clear that for each $(j, i) \in L_{n, p}$

$$
1 \leq j \leq n-1 ; \quad 1 \leq i \leq p-1 ; \quad p(j-1)+(j+1) \leq n(p-i)
$$

Elementary calculations ( $\sqrt{4}$, theorem 3 on p. 403]) show that

$$
\omega_{j, i}:=x^{j-1} d x / y^{p-i}=x^{j-1} y^{i} d x / y^{p}=x^{j-1} y^{i-1} d x / y^{p-1}
$$

is a differential of the first kind on $C$ for each $(j, i) \in L_{n, p}$. This implies easily that the collection $\left\{\omega_{j, i}\right\}_{(j, i) \in L_{n, p}}$ is a basis in the space of differentials of the first kind on $C$.

There is a non-trivial birational $K_{a}$-automorphism of $C$

$$
\delta_{p}:(x, y) \mapsto(x, \zeta y)
$$

Clearly, $\delta_{p}^{p}$ is the identity map and the set of fixed points of $\delta_{p}$ coincides with $B^{\prime}$.
Let $J^{(f, p)}=J(C)=J\left(C_{f, p}\right)$ be the jacobian of $C$. It is a $g$-dimensional abelian variety defined over $K$ and one may view (via Albanese functoriality) $\delta_{p}$ as an element of

$$
\operatorname{Aut}(C) \subset \operatorname{Aut}(J(C)) \subset \operatorname{End}(J(C))
$$

such that $\delta_{p} \neq \mathrm{Id}$ but $\delta_{p}^{p}=\mathrm{Id}$ where Id is the identity endomorphism of $J(C)$. Here $\operatorname{Aut}(C)$ stands for the group of $K_{a}$-automorphisms of $C$, $\operatorname{Aut}(J(C))$ stands for the group of $K_{a}$-automorphisms of $J(C)$ and $\operatorname{End}(J(C))$ stands for the ring of all $K_{a}$-endomorphisms of $J(C)$. As usual, we write $\operatorname{End}^{0}(J(C))=\operatorname{End}^{0}\left(J^{(f, p)}\right)$ for the corresponding $\mathbf{Q}$-algebra $\operatorname{End}(J(C)) \otimes \mathbf{Q}$.

Lemma 3.2. $\operatorname{Id}+\delta_{p}+\cdots+\delta_{p}^{p-1}=0$ in $\operatorname{End}(J(C))$. Therefore the subring $\mathbf{Z}\left[\delta_{p}\right] \subset$ $\operatorname{End}(J(C))$ is isomorphic to the ring $\mathbf{Z}\left[\zeta_{p}\right]$ of integers in the pth cyclotomic field $\mathbf{Q}\left(\zeta_{p}\right)$. The $\mathbf{Q}$-subalgebra $\mathbf{Q}\left[\delta_{p}\right] \subset \operatorname{End}^{0}(J(C))=\operatorname{End}^{0}\left(J^{(f, p)}\right)$ is isomorphic to $\mathbf{Q}\left(\zeta_{p}\right)$.

Proof. See 10, p. 149], [11, p. 458].
Remark 3.3. If $K$ contains $\zeta$ then the Galois modules $\left(\mathbf{F}_{p}^{\Re_{f}}\right)^{00}$ and $\operatorname{ker}\left(\operatorname{Id}-\delta_{p}\right)$ are canonically isomorphic (10, proposition 6.2], 11, proposition 3.2]).

Remark 3.4. Recall that $p$ is odd and assume that $n=\operatorname{deg}(f)$ is divisible by $p$ say, $n=p m$ for some positive integer $m$. Since $n \geq 4$, we conclude that $n \geq 5$.

Let $\alpha \in K_{a}$ be a root of $f$ and $K_{1}=K(\alpha)$ be the corresponding subfield of $K_{a}$. We have $f(x)=(x-\alpha) f_{1}(x)$ with $f_{1}(x) \in K_{1}[x]$. Clearly, $f_{1}(x)$ is a separable
polynomial over $K_{1}$ of degree $p m-1=n-1 \geq 4$. It is also clear that the polynomials

$$
h(x)=f_{1}(x+\alpha), h_{1}(x)=x^{n-1} h(1 / x) \in K_{1}[x]
$$

are separable of the same degree $p m-1=n-1 \geq 4$. The standard substitution

$$
x_{1}=1 /(x-\alpha), y_{1}=y /(x-\alpha)^{m}
$$

establishes a birational isomorphism between $C_{f, p}$ and a curve

$$
C_{h_{1}}: y_{1}^{p}=h_{1}\left(x_{1}\right)
$$

(see [14. p. 3359]). But $\operatorname{deg}\left(h_{1}\right)=p m-1$ is not divisible by $p$. Clearly, this isomorphism commutes with the actions of $\delta_{p}$.

Theorem 3.5. Suppose $n \geq 4$. Assume that $\mathbf{Q}\left[\delta_{p}\right]$ is a maximal commutative subalgebra in $\operatorname{End}^{0}\left(J^{(f, p)}\right)$. Then the center $\mathfrak{C}$ of $\operatorname{End}^{0}\left(J^{(f, p)}\right)$ is a CM-subfield of $\mathbf{Q}\left[\delta_{p}\right]$.

Proof. This is theorem 3.8 of 20.

Theorem 3.6. Suppose $n \geq 4$. Assume that $\mathbf{Q}\left[\delta_{p}\right]$ is a maximal commutative subalgebra in $\operatorname{End}^{0}\left(J^{(f, p)}\right)$. Then $\operatorname{End}^{0}\left(J^{(f, p)}\right)=\mathbf{Q}\left[\delta_{p}\right] \cong \mathbf{Q}\left(\zeta_{p}\right)$ and therefore $\operatorname{End}\left(J^{(f, p)}\right)=\mathbf{Z}\left[\delta_{p}\right] \cong \mathbf{Z}\left[\zeta_{p}\right]$.

Proof. Let $\mathfrak{C}=\mathfrak{C}_{J^{(f, p)}}$ be the center of $\operatorname{End}^{0}\left(J^{(f, p)}\right)$. We know that $\mathfrak{C}$ is a CM-subfield of $E:=\mathbf{Q}\left[\delta_{p}\right]$.

Replacing, if necessary, $K$ by its subfield (finitely) generated over $\mathbf{Q}$ by all the coefficients of $f$, we may assume that $K$ (and therefore $K_{a}$ ) is isomorphic to a subfield of the field $\mathbf{C}$ of complex numbers. So, $K \subset K_{a} \subset \mathbf{C}$. We may also assume that $\zeta=\zeta_{p}$ and consider $C_{(f, p)}$ as complex projective curve and its jacobian $J^{(f, p)}$ as complex abelian variety.

Let $\Sigma=\Sigma_{E}$ be the set of all field embeddings $\sigma: E=\mathbf{Q}\left[\delta_{p}\right] \hookrightarrow \mathbf{C}$. We are going to apply Theorem 2.3 to $Z=J^{(f, p)}$ and $E=\mathbf{Q}\left[\delta_{p}\right]$. In order to do that we need to get some information about the multiplicities

$$
n_{\sigma}=n_{\sigma}(Z, E)=n_{\sigma}\left(J^{(f, p)}, \mathbf{Q}\left[\delta_{p}\right]\right)
$$

Remark 2.2 allows us to do it, using the action of $\mathbf{Q}\left[\delta_{p}\right]$ on the space $\Omega^{1}\left(J^{(f, p)}\right)$ of differentials of the first kind on $J^{(f, p)}$.

Recall that if $\sigma^{\prime}: \mathbf{Q}\left[\delta_{p}\right] \hookrightarrow \mathbf{C}$ is the embedding complex conjugate to $\sigma$ then, by Remark 2.1,

$$
n_{\sigma}+n_{\sigma^{\prime}}=\frac{2 \operatorname{dim}\left(J^{(f, p)}\right)}{p-1},
$$

since $\left[\mathbf{Q}\left[\delta_{p}\right]: \mathbf{Q}\right]=p-1$. Notice also that for each $\sigma: \mathbf{Q}\left[\delta_{p}\right] \hookrightarrow \mathbf{C}$

$$
\Omega^{1}\left(J^{(f, p)}\right)_{\sigma}=\left\{\omega \in \Omega^{1}\left(J^{(f, p)}\right) \mid \delta_{p}(\omega)=\sigma\left(\delta_{p}\right) \omega\right\} .
$$

In other words, $\Omega^{1}\left(J^{(f, p)}\right)_{\sigma}$ is the eigenspace corresponding to the eigenvalue $\sigma\left(\delta_{p}\right)$ of $\delta_{p}$ and $n_{\sigma}$ is the multiplicity of the eigenvalue $\sigma\left(\delta_{p}\right)$.

Let $i<p$ be a positive integer and $\sigma_{i}: \mathbf{Q}\left[\delta_{p}\right] \hookrightarrow \mathbf{C}$ be the embedding which sends $\delta_{p}$ to $\zeta^{-i}$. Obviously, the complex conjugate of $\sigma_{i}$ coincides with $\sigma_{p-i}$. In addition, for each $\sigma$ there exists precisely one $i$ such that $\sigma=\sigma_{i}$. Clearly, $\Omega^{1}\left(J^{(f, p)}\right)_{\sigma_{i}}$ is the eigenspace of $\Omega^{1}\left(J^{(f, p)}\right)$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_{p}$. Therefore $n_{\sigma_{i}}$ coincides with the multiplicity of the eigenvalue $\zeta^{-i}$.

Let $P_{0}$ be one of the $\delta_{p}$-invariant points (i.e., a ramification point for $\pi$ ) of $C_{f, p}\left(K_{a}\right) \subset C_{f, p}(\mathbf{C})$. Then

$$
\tau: C_{f, p} \rightarrow J^{(f, p)}, \quad P \mapsto \operatorname{cl}\left((P)-\left(P_{0}\right)\right)
$$

is an embedding of complex algebraic varieties and it is well-known that the induced map

$$
\tau^{*}: \Omega^{1}\left(J^{(f, p)}\right) \rightarrow \Omega^{1}\left(C_{f, p}\right)
$$

is a $\mathbf{C}$-linear isomorphism obviously commuting with the actions of $\delta_{p}$. (Here cl stands for the linear equivalence class.) This implies that $n_{\sigma_{i}}$ coincides with the dimension of the eigenspace of $\Omega^{1}\left(C_{(f, p)}\right)$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_{p}$.

Remark 3.7. Clearly, if for some positive integer $j$ the differential $x^{j-1} d x / y^{p-i}$ lies in $\Omega^{1}\left(C_{(f, p)}\right)$ then it is an eigenvector of $\delta_{p}$ with eigenvalue $\zeta^{i}$. Now assume that $p$ does not divide $n$. It follows from Remark 3.1 that each $n_{\sigma}=n_{\sigma_{i}}$ could be visualized as the number of interior integer points in $\Delta_{n, p}$ along the corresponding (to $p-i$ ) horizontal line. Elementary calculations show that this number is $\left[\frac{n i}{p}\right]$. This implies that $n_{\sigma_{i}}=\left[\frac{n i}{p}\right]$ for $1 \leq i \leq p-1$. Then $n_{\sigma_{i}}=0$ if and only if $1 \leq i \leq\left[\frac{p}{n}\right]$.

Assume, in addition, that $p<n$. Clearly, in this case the function $i \mapsto n_{\sigma_{i}}=\left[\frac{n i}{p}\right]$ is strictly increasing.

Remark 3.8. Assume that $p$ divides $n$. Then $n \geq 5$ and $n-1 \geq 4$. Clearly, $p$ does not divide $n-1$. Applying Remark 3.4, we get a curve $C_{h_{1}, p}: y_{1}^{p}=h_{1}\left(x_{1}\right)$
with separable polynomial $h_{1}\left(x_{1}\right)$ of degree $n-1$ and a $\delta_{p}$-equivariant birational isomorphism between $C_{f, p}$ and $C_{h_{1}, p}$. This gives us a $\delta_{p}$-equivariant isomorphism

$$
\Omega^{1}\left(C_{f, p}\right) \cong \Omega^{1}\left(C_{h_{1}, p}\right)
$$

Applying Remark 3.7 to $C_{h_{1}, p}$ and $n-1$ (instead of $C_{f, p}$ and $n$ ), we conclude that $n_{\sigma_{i}}=\left[\frac{(n-1) i}{p}\right]$ for $1 \leq i \leq p-1$. Then $n_{\sigma_{i}}=0$ if and only if $1 \leq i \leq\left[\frac{p}{n-1}\right]$.

Assume, in addition, that $n \neq p$. Clearly, in this case $n-1>p$ and the function $i \mapsto n_{\sigma_{i}}=\left[\frac{(n-1) i}{p}\right]$ is strictly increasing.

Proposition 3.9. (i) let us assume that $p>n$. Then $n_{\sigma}=0$ if and only if $\sigma=\sigma_{i}$ with $1 \leq i \leq\left[\frac{(p-1)}{n}\right]$.
(ii) let us assume that $p=n$. Then $n_{\sigma}=0$ if and only if $\sigma=\sigma_{i}$ with $i=1$.

Proof of Proposition 3.9. First, assume that $p>n$. Clearly, $p$ does not divide $n$ and therefore $\left[\frac{p}{n}\right]=\left[\frac{p-1}{n}\right]$. Now the assertion (i) follows from Remark 3.7.

Now assume that $n=p$. By Remark 3.8, $n_{\sigma_{i}}=0$ if and only if $1 \leq i \leq\left[\frac{p}{n-1}\right]$. But $\left[\frac{p}{n-1}\right]=\left[\frac{p}{p-1}\right]=1$.

Proposition 3.10. Let us assume that $p<n$. If $\sigma, \iota$ are two embeddings $\mathbf{Q}\left[\delta_{p}\right] \hookrightarrow$ $\mathbf{C}$ then $n_{\sigma}=n_{\iota}$ if and only if $\sigma=\iota$.

Proof of Proposition 3.1d. First assume that $p$ does not divide $n$. Then the assertion follows from (the last sentence of) Remark 3.7.

Now assume that $p$ divides $n$. Then the assertion follows from (the last sentence of) Remark 3.8.

End of the proof of Theorem 3.6. If $\mathfrak{C}=\mathbf{Q}\left[\delta_{p}\right]$ then we are done, since $\mathbf{Q}\left[\delta_{p}\right]$ is a maximal commutative subalgebra in $\operatorname{End}^{0}\left(J^{(f, p)}\right)$. Assume that $\mathfrak{C} \neq \mathbf{Q}\left[\delta_{p}\right]$. Our goal is to get a contradiction.

Clearly, $\mathbf{Q}\left[\delta_{p}\right] / \mathbf{Q}$ is a Galois extension. It follows from Theorem 2.3 and Remark 2.2 (applied to $Z=J^{(f, p)}$ and $E=\mathbf{Q}\left[\delta_{p}\right]$ ) that there exists a non-trivial field automorphism $\kappa: \mathbf{Q}\left[\delta_{p}\right] \rightarrow \mathbf{Q}\left[\delta_{p}\right]$ such that for all $\sigma \in \Sigma$

$$
n_{\sigma}=n_{\sigma \kappa}
$$

Clearly, there exists an integer $m$ such that $1<m<p$ and $\kappa\left(\delta_{p}\right)=\delta_{p}^{m}$.
First, assume that $n>p$. It follows from Proposition 3.10 that $\sigma \kappa=\sigma$ which could not be the case, since $\kappa$ is not the identity map. This contradiction proves the Theorem in the case of $n>p$.

Second, assume that $n=p$. It follows from Proposition 3.9(ii) that $\sigma_{1} \kappa=\sigma_{1}$ which, by the same token, leads to a contradiction.

Third, assume that $p>n$. It follows from Proposition 3.9(i) that the map $\sigma \mapsto \sigma \kappa$ permutes the set $\left\{\sigma_{i} \left\lvert\, 1 \leq i \leq\left[\frac{(p-1)}{n}\right]\right.\right\}$. Since $\kappa\left(\delta_{p}\right)=\delta_{p}^{m}, \sigma_{i} \kappa\left(\delta_{p}\right)=$ $\zeta^{-i m}$. This implies that multiplication by $m$ in $\mathbf{F}_{p}^{*}$ leaves invariant the subset $A:=\left\{i \bmod p \in \mathbf{F}_{p} \left\lvert\, 1 \leq i \leq\left[\frac{(p-1)}{n}\right]\right.\right\}$. This implies that

$$
m=m \cdot 1 \leq\left[\frac{(p-1)}{n}\right] \leq \frac{(p-1)}{4}
$$

Let us consider the arithmetic progression consisting of the $m$ integers $\left[\frac{(p-1)}{n}\right]+$ $1, \ldots,\left[\frac{(p-1)}{n}\right]+m$ with difference 1 . All its elements lie between $\left[\frac{(p-1)}{n}\right]+1$ and

$$
\left[\frac{(p-1)}{n}\right]+m \leq 2\left[\frac{(p-1)}{n}\right] \leq 2 \frac{(p-1)}{4}=\frac{(p-1)}{2}<p-1
$$

Clearly, there exists a positive integer $r \leq m$ such that $\left[\frac{(p-1)}{n}\right]+r$ is divisible by $m$, i.e., there is a positive integer $d$ such that $m d=\left[\frac{(p-1)}{n}\right]+r$. Since $\left[\frac{(p-1)}{n}\right] \geq m \geq 2$, we have $d \leq\left[\frac{(p-1)}{n}\right]$ but $m d=\left[\frac{(p-1)}{n}\right]+r \leq\left[\frac{(p-1)}{n}\right]+m<p-1$. This implies that $A$ is not invariant under multiplication by $m$ which gives the desired contradiction.

## 4. Jacobians and their endomorphism Rings

Recall that $K$ is a field of characteristic zero, $K_{a}$ is its algebraic closure. Suppose $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots, $\mathfrak{R}_{f} \subset K_{a}$ is the set of its roots, $K\left(\Re_{f}\right)$ is its splitting field. Let us put

$$
\operatorname{Gal}(f)=\operatorname{Gal}\left(K\left(\Re_{f}\right) / K\right) \subset \operatorname{Perm}\left(\Re_{f}\right)
$$

Theorem 4.1 (corollary 5.3 of 20). Let $p$ be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\operatorname{Gal}(f)=\mathbf{S}_{n}$ or $\mathbf{A}_{n}$ then $\mathbf{Q}\left[\delta_{p}\right]$ is a maximal commutative subalgebra in $\operatorname{End}^{0}\left(J^{(f, p)}\right)$ and the center of $\operatorname{End}^{0}\left(J^{(f, p)}\right)$ is a CM-subfield of $\mathbf{Q}\left[\delta_{p}\right]$.

Combining Theorems 4.1 and 3.6, we obtain the following statement.

Theorem 4.2. Let $p$ be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\operatorname{Gal}(f)=\mathbf{S}_{n}$ or $\mathbf{A}_{n}$ then $\operatorname{End}^{0}\left(J^{(f, p)}\right)=\mathbf{Q}\left[\delta_{p}\right]$ and therefore $\operatorname{End}\left(J^{(f, p)}\right)=\mathbf{Z}\left[\delta_{p}\right] \cong \mathbf{Z}\left[\zeta_{p}\right]$.

Clearly, Theorem 1.1 is a special case of Theorem 4.2.

Example 4.3. Suppose $L=\mathbf{C}\left(z_{1}, \cdots, z_{n}\right)$ is the field of rational functions in $n$ independent variables $z_{1}, \cdots, z_{n}$ with constant field $\mathbf{C}$ and $K=L^{\mathbf{S}_{n}}$ is the subfield of symmetric functions. Then $K_{a}=L_{a}$ and

$$
f(x)=\prod_{i=1}^{n}\left(x-z_{i}\right) \in K[x]
$$

is an irreducible polynomial over $K$ with Galois group $\mathbf{S}_{n}$. Let $C$ be a smooth projective model of the $K$-curve $y^{p}=f(x)$ and $J(C)$ its jacobian. It follows from Theorem 4.2 that if $n \geq 5$ then the ring of $L_{a}$-endomorphisms of $J(C)$ is $\mathbf{Z}\left[\zeta_{p}\right]$. In particular, the abelian variety $J(C)$ is absolutely simple. When $p=3$ and $3 \mid n$ the absolute simplicity of $J(C)$ was proven in (15, p. 107]).

Example 4.4. Let $h(x) \in \mathbf{C}[x]$ be a Morse polynomial of degree $n \geq 5$. This means that the derivative $h^{\prime}(x)$ of $h(x)$ has $n-1$ distinct roots $\beta_{1}, \cdots \beta_{n-1}$ and $h\left(\beta_{i}\right) \neq h\left(\beta_{j}\right)$ while $i \neq j$. (For example, $x^{n}-x$ is a Morse polynomial.) Let $K=\mathbf{C}(z)$ be the field of rational functions in variable $z$ with constant field $\mathbf{C}$ and $K_{a}$ its algebraic closure. Then a theorem of Hilbert ([13, theorem 4.4.5, p. 41]) asserts that the Galois group of $h(x)-z$ over $k(z)$ is $\mathbf{S}_{n}$. Let $C$ be a smooth projective model of the $K$-curve $y^{p}=h(x)-z$ and $J(C)$ its jacobian. It follows from Theorem 4.2 that the ring of $K_{a}$-endomorphisms of $J(C)$ is $\mathbf{Z}\left[\zeta_{p}\right]$. In particular, the abelian variety $J(C)$ is absolutely simple.

We refer the reader to [18, 19, 20, 22] for the definition and basic properties of very simple representations.

Theorem 4.5. Suppose $p$ is an odd prime, $n \geq 5$ and $K$ contains a primitive $p$ th root of unity. If the $\operatorname{Gal}(f)$-module $\left(\mathbf{F}_{p}^{\Re_{f}}\right)^{00}$ is very simple then $\mathbf{Q}\left[\delta_{p}\right]$ coincides with its own centralizer in $\operatorname{End}^{0}\left(J^{(f, p)}\right)$.

Proof. See theorem 5.2 of 20.
Theorem 4.6. Suppose $p$ is an odd prime, $n \geq 5$ and $K$ contains a primitive $p$ th root of unity. If the $\operatorname{Gal}(f)$-module $\left(\mathbf{F}_{p}^{\mathfrak{R}_{f}}\right)^{00}$ is very simple then $\operatorname{End}^{0}\left(J^{(f, p)}\right)=$ $\mathbf{Q}\left[\delta_{p}\right]$ and therefore $\operatorname{End}\left(J^{(f, p)}\right)=\mathbf{Z}\left[\delta_{p}\right] \cong \mathbf{Z}\left[\zeta_{p}\right]$.

Proof. It is an immediate corollary of Theorem 4.5 combined with Theorem 3.6.

## 5. Corrigendum to 20

Remark 2.1 on p. 94, the last assertion. In general, it is not necessarily true that $G$ is doubly transitive [3, Beispiel 2c], [8]. However, it becomes true if one
assumes additionally that either $p$ does not divide $n$ or $G$ is transitive and $p$ is an odd number dividing $n$ (33, Satz 4a and Satz 11], [20, lemma 2.4]).

Lemma 2.4 on p. 95. Its assertion is essentially contained in Satz 4a of [3].
Remark 2.5 on p. 95. Its assertion is essentially Hilffsatz 3b of [3].
Sections 1,3 and 5 . Everywhere $\mathbf{Q}\left(\delta_{p}\right)$ means $\mathbf{Q}\left[\delta_{p}\right]$. (However, it does not make a difference, since $\mathbf{Q}\left[\delta_{p}\right]$ is a field.)

## References

[1] P. Deligne, Hodge cycles on abelian varieties (notes by J.S. Milne). Lecture Notes in Math., vol. 900 (Springer-Verlag, 1982), pp. 9-100.
[2] J. de Jong and R. Noot, Jacobians with complex multiplications. In: Arithmetic algebraic geometry (eds. G. van der Geer, F. Oort and J. Steenbrink). Progress in Math., vol. 89 (Birkhäuser, 1991), pp. 177-192.
[3] M. Klemm, Über die Reduktion von Permutationsmoduln. Math. Z. 143 (1975), 113-117.
[4] J. K. Koo, On holomorphic differentials of some algebraic function field of one variable over C. Bull. Austral. Math. Soc. 43 (1991), 399-405.
[5] B. Moonen and Yu. G. Zarhin, Weil classes on abelian varieties. J. reine angew. Math. 496 (1998), 83-92.
[6] B. Mortimer, The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. (3) 41 (1980), 1-20.
[7] D. Mumford, Abelian varieties, 2nd edn (Oxford University Press, 1974).
[8] P. M. Neumann, Review of [3, MR $52 \# 544$.
[9] K. Ribet, Hodge classes on certain abelian varieties. Amer. J. Math. 105 (1983), 523-538.
[10] B. Poonen and E. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line. J. reine angew. Math. 488 (1997), 141-188.
[11] E. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann. 310 (1998), 447-471.
[12] I. Schur, Gleichungen ohne Affect. Sitz. Preuss. Akad. Wiss. 1930, Physik-Math. Klasse 443449 (=Ges. Abh. III, 191-197).
[13] J.-P. Serre, Topics in Galois Theory (Jones and Bartlett Publishers, 1992).
[14] C. Towse, Weierstrass points on cyclic covers of the projective line. Trans. Amer. Math. Soc. 348 (1996), 3355-3377.
[15] H. Völklein, Cyclic covers of $\mathbf{P}^{1}$ and Galois actions on their division points. Contemporary Math. 186 (1994), 91-107.
[16] Yu. G. Zarhin, Weights of simple Lie algebras in the cohomology of algebraic varieties. Izv. Akad. Nauk SSSR Ser. Mat. 48 (1984), 264-304; English translation: Math. USSR Izv. 24 (1985), 245-281.
[17] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7 (2000), 123-132.
[18] Yu. G. Zarhin, Hyperelliptic jacobians and modular representations. In: Moduli of abelian varieties (eds. C. Faber, G. van der Geer and F. Oort). Progress in Math., vol. 195 (Birkhäuser, 2001), pp. 473-490.
[19] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication in positive characteristic. Math. Res. Letters 8 (2001), 429-435.
[20] Yu. G. Zarhin, Cyclic covers of the projective line, their jacobians and endomorphisms. J. reine angew. Math. 544 (2002), 91-110.
[21] Yu. G. Zarhin, Endomorphism rings of certain jacobians in finite characteristic. Matem. Sbornik 193 (2002), issue 8 (Russian), to appear.
[22] Yu. G. Zarhin, Very simple 2-adic representations and hyperelliptic jacobians; available at http://arXiv.org/abs/math.AG/0109014; Moscow Math. J. 2 (2002), issue 2, to appear.

